NSCC / SageSync — antivirus exclusions for IT

> **PDF for IT:** NSCC_ANTIVIRUS_EXCLUSIONS.pdf — live: https://northstar-courier-command.web.app/docs/NSCC_ANTIVIRUS_EXCLUSIONS.pdf

Give this page to the person who manages antivirus / EDR on SERVER2019. Host: SERVER2019 (Sage 300 CRE + NSCC middleware) **Product:** NorthStar Courier Command (NSCC) Sage bridge **Why:** Real-time scanners often quarantine or lock Python, `.py`, scheduled-task launches, Firestore service-account JSON, and ODBC traffic. That stops watch/poll, so NSCC cannot push AR/payroll staging into Sage.

Do **not** exclude the whole `C:\` drive. Only the paths and processes below.

---

1. Folder exclusions (required)

Add these as **path / folder** exclusions (real-time + on-access scan). Include subfolders.

`D:\SageSync\`	Middleware, scripts, Traffic Cop web UI, logs, secrets
`D:\SageSync\sage_middleware\`	`run.py` and ODBC bridge libraries
`D:\SageSync\scripts\`	Watch / poll / install scheduled tasks
`D:\SageSync\logs\`	Watch/poll/WORM logs (written continuously)
`D:\SageSync\secrets\`	Firebase service-account JSON (AV often flags this)
`D:\SageSync\web\`	Local Traffic Cop UI (`http://localhost:8766/`)
`D:\projects\nscc\`	Git clone used by `NSCC_RepoPull` / `update_nscc_server.ps1`

If Python is **not** the Microsoft Store stub, also exclude the real install, for example:

`C:\Python312\` or `C:\Program Files\Python3xx\`	Official python.org install
`%LOCALAPPDATA%\Programs\Python\`	Per-user python.org install

Confirm on the server with: `where python` and `py -3 -c "import sys; print(sys.executable)"`.

---

2. Process exclusions (required)

`python.exe` (and `pythonw.exe` if present)	`sage_middleware\run.py` watch + poll
`py.exe`	Windows Python launcher (`py -3`) used by `START_SAGE_WATCH.bat`

`powershell.exe` when started from `D:\SageSync\scripts\`	Poll / daily / repo-update tasks
`cmd.exe` when starting `D:\SageSync\scripts\START_SAGE_WATCH.bat`	Continuous watch loop

Prefer **path-scoped** process exclusions (process + working directory under `D:\SageSync`) if the AV product supports it. Do not globally exclude all `powershell.exe` on the server if policy forbids it — then use folder exclusions in section 1 plus allow-list the scheduled tasks below.

---

3. Scheduled tasks that must be allowed to run

These are installed by `D:\SageSync\scripts\install_scheduled_tasks.ps1` (run as Administrator). AV / exploit-guard must not block them.

`NSCC_SageWatch`	At startup, continuous	`cmd.exe /c D:\SageSync\scripts\START_SAGE_WATCH.bat` → `python … sync watch`
`NSCC_SagePoll`	Every 5 minutes	`powershell.exe -File D:\SageSync\scripts\schedule_sage_poll.ps1 -Env both`
`NSCC_SageDaily`	Daily 02:30	Same poll script, full inbound
`NSCC_RepoPull`	Daily 03:15	`update_nscc_server.ps1` (git pull + overlay)

Also allow **WORM verify** if installed (`worm_verify.py` / `INSTALL_WORM_ALERT.ps1`) — same `python.exe` + `D:\SageSync\` folders.

---

4. Network allow-list (if the AV/firewall filters outbound)

`*.googleapis.com` / `*.firebaseio.com` / `firestore.googleapis.com`	Firestore queue + masters
`northstar-courier-command.firebaseapp.com`	Firebase Auth / project
`github.com` / `*.github.com` (HTTPS 443)	`NSCC_RepoPull` git update
Local ODBC to Sage 300 CRE (Pervasive / Actian)	Staging `INSERT` into `NSCC_JC_Staging` / `NSCC_PR_Staging`

Traffic Cop UI is **localhost only** (`127.0.0.1:8766`). No inbound internet port is required for that page.

---

5. What success looks like

On SERVER2019, after exclusions:

```
python D:\SageSync\sage_middleware\run.py env test --env sandbox --use-firestore --publish
```

Bridge health should **PASS**. Watch/poll tasks should stay **Running** and must not disappear a few seconds after start (classic AV kill).

---

6. Contact / product

- - App: NorthStar Courier Command
- - Firebase project: `northstar-courier-command`
- - Server home: `D:\SageSync`
- - Ops detail: `D:\SageSync\web\docs\SERVER_OPERATIONS.md` (or repo `server/sage_traffic_cop/public/docs/SERVER_OPERATIONS.md`)